

UNITED STATES DISTRICT COURT

for the
Middle District of Tennessee

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Residence at [REDACTED], TN; all
other associated storage areas & units; and white 2017
Mercedes E43 registered to [REDACTED]

Case No. 19-mj-4221

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Middle District of Tennessee
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before August 21, 2019 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.


The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to United States Magistrate Judge Barbara Holmes
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued:

8/7/19 5:45pm


Judge's signature

City and state:

Nashville, Tennessee

United States Magistrate Judge Alistair E. Newbern

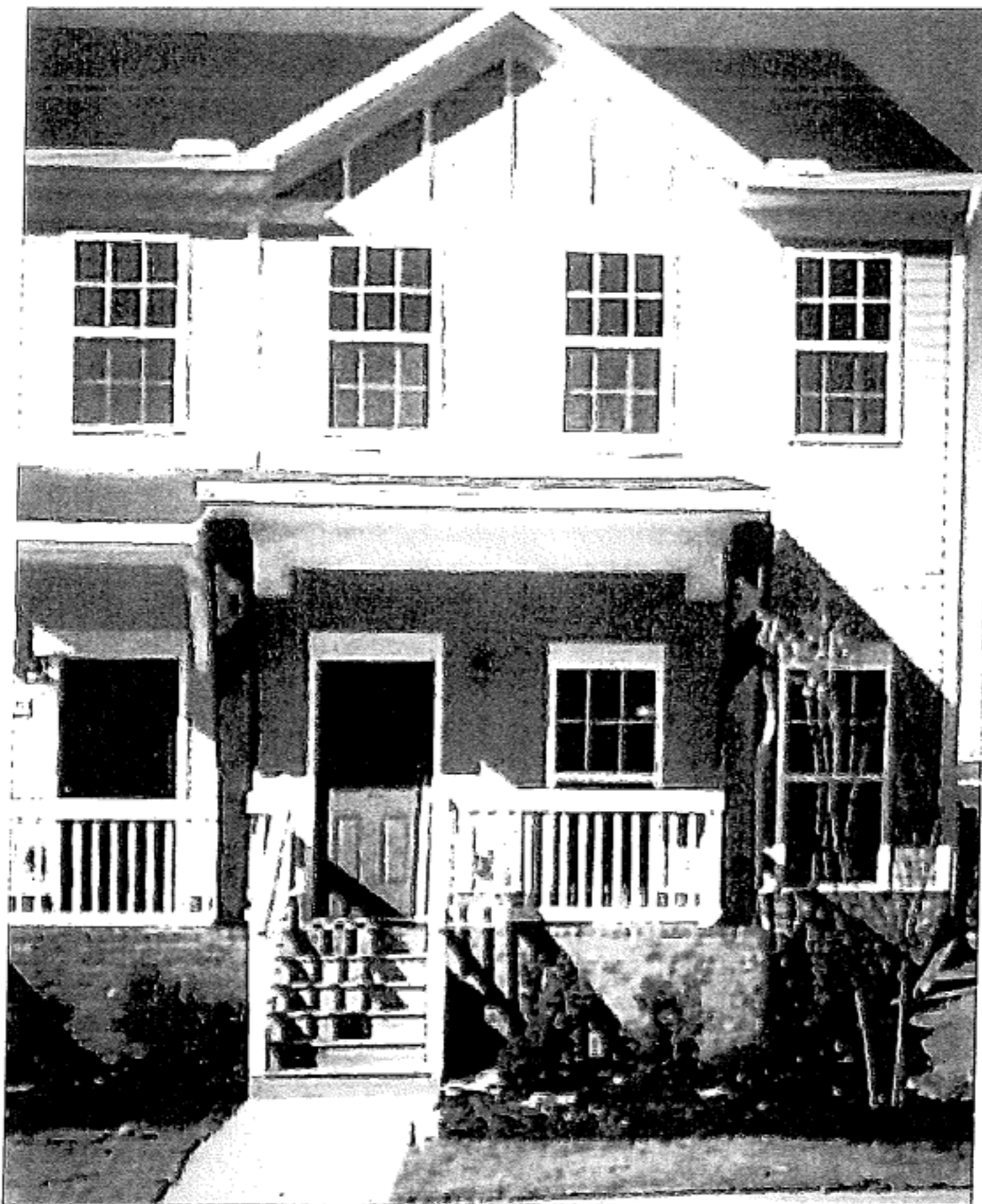
Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is as follows:

1. [REDACTED] more particularly described as a two story town home with gray siding, a blue door, wooden steps up to a small front porch with white railing, and a sidewalk leading up to the stairs:



2. White 2017 Mercedes E43, with temporary tag [REDACTED] that has an expiration date of September 5, 2019, and registered to [REDACTED] Antioch, Tennessee 37013.

ATTACHMENT B

Property to be seized

1. All records relating to violations of Title 18, United States Code, Section 1030, those violations involving [REDACTED] and occurring between on or about February 8, 2019, and August 7, 2019, including:

- a. Company A's computer, TargetPC;
- b. Records and information relating to access of Company A's networks, systems, and computers;
- c. Records and information relating to Company A;
- d. Records and information relating to the identity or location of any co-conspirators;
- e. Records and information relating to the proton e-mail account used in the extortion;
- f. Records and information relating to online communications with ExpressVPN;
- g. Records and information relating to malicious software.

2. Computers and storage media used as a means to commit the violations described above, including downloading confidential materials without authorization in violation of 18 U.S.C. § 1030(a)(2).

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing

history, user profiles, email, email contacts, "chat," instant messaging logs, texts, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;

- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - m. contextual information necessary to understand the evidence described in this attachment.
4. Routers, modems, and network equipment used to connect computers to the Internet.
 5. The person of [REDACTED] for purposes of obtaining all evidence described herein, as long as [REDACTED] is present at the PREMISES.
 6. The [REDACTED] for purposes of obtaining all evidence described herein, including proceeds of the fraudulently obtained funds.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search of the Subject Premises described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face those same individuals and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

UNITED STATES DISTRICT COURT

for the
Middle District of TennesseeIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Residence at [REDACTED] all
other associated storage areas & units; and white 2017
Mercedes E43 registered to [REDACTED]

Case No. 19-mj-4221

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Middle District of Tennessee, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. 1030

Fraud and Related Activity in Connection with Computers

The application is based on these facts:

See Attachment C

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

FBI Special Agent Casper W. Cromwell

Printed name and title

Sworn to before me and signed in my presence.

Date: 08/07/2019



Judge's signature

City and state: Nashville, Tennessee

United States Magistrate Judge Alistair E. Newbern

Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is as follows:

1. [REDACTED], more particularly described as a two story town home with gray siding, a blue door, wooden steps up to a small front porch with white railing, and a sidewalk leading up to the stairs:



2. White 2017 Mercedes E43, with temporary tag [REDACTED] that has an expiration date of September 5, 2019, and registered to [REDACTED], Antioch, Tennessee 37013.

ATTACHMENT B

Property to be seized

1. All records relating to violations of Title 18, United States Code, Section 1030, those violations involving [REDACTED] and occurring between on or about February 8, 2019, and August 7, 2019, including:

- a. Company A's computer, TargetPC;
- b. Records and information relating to access of Company A's networks, systems, and computers;
- c. Records and information relating to Company A;
- d. Records and information relating to the identity or location of any co-conspirators;
- e. Records and information relating to the proton e-mail account used in the extortion;
- f. Records and information relating to online communications with ExpressVPN;
- g. Records and information relating to malicious software.

2. Computers and storage media used as a means to commit the violations described above, including downloading confidential materials without authorization in violation of 18 U.S.C. § 1030(a)(2).

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing

history, user profiles, email, email contacts, "chat," instant messaging logs, texts, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;

1. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.
4. Routers, modems, and network equipment used to connect computers to the Internet.
5. The person of [REDACTED] for purposes of obtaining all evidence described herein, as long as [REDACTED] is present at the PREMISES.
6. The 2017 Mercedes E43 for purposes of obtaining all evidence described herein, including proceeds of the fraudulently obtained funds.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search of the Subject Premises described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face those same individuals and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

Attachment C
Statement in Support of Search Warrant

I, Casper W. Cromwell, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as [REDACTED], Antioch, Tennessee 37013, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since March 1, 2009. I currently am assigned to conduct cybercrime investigations that involve numerous cases of computer intrusion, Internet fraud, and the theft of intellectual property.

3. The facts in this affidavit come from my personal observations, my training and experience, the review of documents and records, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(a)(4), and 1030(a)(5)(A) have been committed by one or more unknown persons. Title 18, United States Code, Section 1030(a)(2)(C) makes it an offense to intentionally access a computer without authorization, or to exceed authorized access, and to thereby obtain information from any protected computer. Title 18, United States Code, Section 1030(a)(4) makes it an offense for anyone knowingly and with intent to defraud to access a protected computer without authorization, or to exceed authorized access, and by means of such conduct further the intended fraud and obtain

anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period. Title 18, United States Code, Section 1030(a)(5)(A) makes it an offense to knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer.

PROBABLE CAUSE

5. On August 1, 2019, a Special Agent with the SA Victor Rodriguez met with representatives from Target Wireless Devices, a company in the technology sector with operations in the Metropolitan Nashville area, regarding developing circumstances surrounding the compromise of confidential corporate data. Three high level security executives provided an overview of the situation and their actions to date, as described below.

6. On July 31, 2019, seven executives of Company A received an email or text from an unidentified actor, using a proton email account, claiming to have over 100TB of sensitive data from Company A data, supposedly including thousands of employees' social security number, addresses, bank routing information, bank account numbers, and other sensitive information. The attacker(s) also claimed to have over a million customers' names, addresses, phone numbers, and account numbers; thousands of recorded calls; hundreds of financial documents (P&L, budgets, bank account balances) dating back as far as 2010; customer relations management system documents; and all of the company's training materials. The subject threatened that if the company did not transfer the equivalent of \$350,000 into a specific Bitcoin ("BTC") wallet within 24 hours, he would leak the data to top national newspapers and online technology publications; competitors of Company A; top executives of other well-known technology companies; and employees and board of director members of Company A. The suspect(s) concluded his email by stating that his

only motivation was money. He attached samples of the documents he had claimed to have, including the social security numbers for 18 current and former employees, and a link to a Mega account that appears to contain 20GB of company-related documents.

7. Company A staff reviewed the information posted at the Mega account link, which had been uploaded to that file sharing site in mid-April 2019. The staff confirmed that the data contained confidential information obtained from an internal file server belonging to Company A. The emails also contained the social security account numbers for several current and former employees.

8. Company A launched an investigation and reported the intrusion to the FBI. Company A agreed to pay the suspect(s) \$50,000 per day, rather than a single lump sum, in an effort to protect the company data. The company has been making these payment by depositing the money into a BTC wallets provided by the suspects(s). After each deposit, the company sends an email to the proton email address notifying the suspect(s) of the deposit and asking for confirmation of receipt. During the email exchange, the suspect(s) have included social security numbers for approximately 20 additional current and former employee. The suspect(s) also promised to provide a detailed "essay" explaining how they obtained the data. To date, the company has transferred approximately \$300,000 to the BTC wallets.

9. Company A has reviewed all of the stolen information provided by the subject(s) and determined it to be authentic, i.e. the data matched internal Company A data.

10. During its internal investigation, Company A discovered suspicious network and system activity related to this incident that appears to be linked to a former employee, [REDACTED] who was terminated for performance-related reasons. [REDACTED] last day on premises was March 7, 2019, and his termination was effective March 14, 2019. [REDACTED] had been employed by

Company A from 2010 to March 14, 2019. During his time with Company A, his responsibilities had included website development, project management, planning, and directing resources within the customer solutions team. Employee records indicate he had self-identified technical expertise abilities including but not limited to: Agile Methodologies, CSS3, HTML5, Photoshop, Sharepoint, software quality assurance testing, and user experience in product development and testing. Burk's last address of record with Company A was [REDACTED] Antioch, Tennessee 37013. Additionally, he provided a personal email address of [REDACTED]

11. Company A has observed numerous incidents that occurred prior to [REDACTED] termination of him sending emails from his work account to his personal gmail account that appeared to be test messages, in that they contained no substantive data and consisted of a short string of random letters.

12. Through log and system analysis, the Company A security team has ascertained that a company laptop (hereinafter "TargetPC"), currently is unaccounted for from the Company A environment. The records show that [REDACTED] logged into TargetPC using his Company A account on February 6, 2019, which was the last login prior to the computer's disappearance.

13. Company A's network records numerous data items from machines that connect to its networks, including the missing computer "TargetPC." For example, on February 7, 2019, Company A network logs show that TargetPC connected remotely to the Company A virtual private network (VPN) using the user account of another employee, MS, (hereinafter "MS_Account"). This account is assigned to a current Company A employee, who was interviewed and denied having used TargetPC to access the Company A network. This employee's denial that she used TargetPC is substantiated by logs showing concurrent login activity from

geographically disparate locations and that one of the sessions was at Company A during the employee's shift. The other login location was unknown due to the use of VPN, which masks location information. Based on this collective information, it appears that the MS_Account was compromised, in that it was used by another user with physical access to TargetCP.

14. After Company A determined that the TargetPC was unaccounted for, Company A logs show that connections to Company A's network from TargetPC using the MS_Account included connections from IP address 98.193.239.84. Company A network logs also show that the IP address 98.193.239.84 had been used by [REDACTED] credentials prior to his termination, over an extended time to remotely access Company A systems, from the laptop assigned to him by Company A.

15. The investigation has revealed that 98.193.239.84 belongs to Comcast Corporation in Nashville. Comcast reports that from on or before February 8, 2019 to at least March 14, 2019, this IP address was assigned to [REDACTED] Antioch, Tennessee 37013.

16. Company A network logs also show that the TargetPC had been used to log into the MS_Account using multiple source IPs owned by ExpressVPN, a virtual private network service that makes true source internet address identification difficult. The use of these ExpressVPN source IPs began March 12, 2019, after [REDACTED] left the company premises but before his termination effective date. Significantly, between March 12, 2019, and March 14, 2019 ([REDACTED] last day of employment with the company), the TargetPC was used to access MS_Account remotely, at which time the user accessed Company A file servers containing approximately 80GB of data. During those three days, logs show that four external storage devices were connected to TargetPC, suggesting that data was exfiltrated from company systems and transferred to external

devices. This is supported by the finding that the data in the Mega account forensically matched a subset of this data accessed between March 12 and 14 from TargetPC.

17. On July 16, 2019, MS change her password for her account, the MS_Account, from her work computer pursuant to company policy that requires passwords be changed at least every 90 days.

18. Less than seven hours after the suspect(s) sent the demand email/texts on July 31, 2019, an individual tried to log remotely into the company's systems multiple times using the MS_Account on TargetPC. That account was automatically locked due to multiple incorrect authentication attempts. During this same timeframe, there was no network activity from MS's computer at Company A.

19. Closed source database searches for [REDACTED] identified three possible residences:

[REDACTED], Antioch, Tennessee 37013,
[REDACTED] Antioch, Tennessee 37013, and
[REDACTED] Antioch, Tennessee 37013.

On August 5, 2019, I obtained a pen trap and trace for the MAC addresses of Company A's stolen computer, as well as the personal computer, a Mac computer, that [REDACTED] had used to access Company A's network. A MAC address is assigned by the manufacturer and is a unique number for a device. Passive surveillance, however, has had negative results at these addresses.

20. During traditional surveillance on the morning of August 6, 2019, however, a law enforcement officer identified a 2018 Nissan Sentra at [REDACTED], Antioch, Tennessee 37013. The vehicle is registered to [REDACTED]. An open source social media search located a Facebook account for [REDACTED] in which she identifies [REDACTED] as her boyfriend. A closed

records search lists the residents at that location as [REDACTED]

and [REDACTED]

21. In the afternoon, a law enforcement officer observed a 2017 Mercedes E43, with a temporary license plate and registered to [REDACTED] Antioch, Tennessee. The vehicle had been purchased that day and was parked behind the residence. A law enforcement officer observed [REDACTED] getting into the 2017 Mercedes E43 and driving away.

22. While [REDACTED] was driving the vehicle, Company A made a payment of \$5,000 to the subject. Shortly after the transfer of funds, the surveillance team noted that [REDACTED] picked up his cell phone and typed on it. A few minutes later, Company A received an email from the subject's proton email account stating that only \$5,000 had been received and if the additional \$45,000 wasn't received that day, then the subject would release the stolen data. The remaining \$45,000 was transferred to the BTC account.

23. Based on the negative results from the pen trap, the events in the previous paragraph, and the sending of text messages on July 31, 2019, I believe that [REDACTED] is using his phone to communicate with Company A executives. As such, we request permission to seize [REDACTED] cellular telephone, whether it is in his residence, on his person, or in his vehicle.

24. Additionally, based on the subject's use of BTC, we are seeking to seize evidence of cryptocurrency used to deposit the funds from Company A, as well as any cryptocurrency or other accounts to which the original funds were transferred, including banking documents.

25. Finally, we seek to search the 2017 Mercedes E43 purchased on August 6, 2019, to determine how the vehicle was purchased or any other documentation related to the criminal conduct detailed herein.

TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

27. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

SUPPLEMENTAL CRYPTOCURRENCY AFFIDAVIT LANGUAGE TO SUPPORT RESIDENTIAL SEARCH

28. Based on my training and experience, I know that individuals involved in theft and fraudulent activities often maintain records (including financial records, receipts, notes, ledgers, mail, tax records, and other papers) related to their crimes, and that these records are often maintained at places where the individuals can have ready access to them, including their residence. In my training and experience, I also know that individuals who have committed crimes using computers, such as the subject(s) in this case, often keep records of their crimes in digital or electronic format, such as on a computer, and that computers are often stored in a residence.

29. It should be noted that because the subject(s)'s crimes involved the use of virtual currency, the items to be seized could be stored almost anywhere within a residence, in both physical and electronic formats. For example, Attachment B seeks bitcoin addresses, bitcoin private keys, bitcoin root keys, PGP keys, and passwords. These pieces of data comprise long and complex character strings, and in my training and experience, I know that many virtual currency users write down or otherwise record and store such items because they are too long to commit to memory. As such, these keys, passwords, and addresses may be documented in writing and

secreted anywhere within a residence. For all of the foregoing reasons, your affiant respectfully submits that probable cause exists to believe that such records, data, and documents will be found within the PREMISES, including in computers or on other devices that store electronic data.

30. *Probable cause.* I submit that computers, cellular telephones, or storage media is found on the PREMISES, there is probable cause to believe records of the subject(s)'s fraudulent activity will be stored on those devices and/or media, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system

configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

31. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronic files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how electronics were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence could be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the

suspect(s). For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer

and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

32. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an

image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

33. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

34. *Unlocking the device(s) with biometric features.* The warrant I am applying for would permit law enforcement agents to obtain from the person of [REDACTED] (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometric access subject to seizure, and attempting to access data contained in the device, pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s) or access data contained therein. The grounds for this request are as follows:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition

features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
- c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple’s “Face ID”) have different names but operate similarly to Trusted Face.
- d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the

infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

- e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- f. As discussed in this Statement, I have reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.
- g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from

other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

- h. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from [REDACTED] the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s) found at the PREMISES; (2) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s), or access data contained within the Device(s), in order to search the contents as authorized by this warrant.
- i. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s) or access data contained within the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents

in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

35. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

FORFEITURE

36. This application requests the issuance of a warrant under 21 U.S.C. § 853(f) authorizing the seizure of property subject to forfeiture. This is appropriate because: (1) there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture, and (2) an order under 21 U.S.C. § 853(e) may not be sufficient to assure the availability of the property for forfeiture. There is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture, because 18 U.S.C. § 1030(i)(1)(B) provides that the defendant's "property, real or personal, constitution or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation" shall be forfeited to the United States.

CONCLUSION

37. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.